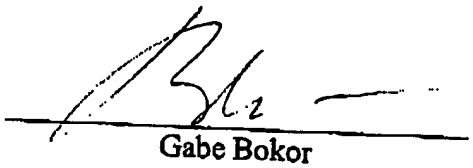
ACCURAPID
Translation Services, Inc. / AB Typesetting

Affidavit of Accuracy

I, Gabe Bokor, of Accurapid Translation Services, Inc., hereby certify that the attached translation from German to English, entitled VERFAHREN ZUR DURCHFÜHRUNG EINES BUCHUNGSVORGANGES [METHOD OF PERFORMING A POSTING] was performed by Accurapid Translation Services, Inc. I also certify that I carefully compared the translation to the original, and that, to the best of my knowledge and belief, it is an accurate and full translation of the original text, and that I am a competent translator in the German and English languages.

Poughkeepsie, September 26, 2005



Gabe Bokor

806 Main Street, Poughkeepsie, New York 12603-1829, USA
Phone: (845) 473-4550 • Fax: (845) 473-4554 • http://accurapid.com • inquiries@accurapid.com

Verfahren zur Durchführung eines Buchungsvorganges

Die Erfindung betrifft ein Verfahren zur Durchführung eines Buchungsvorganges auf einem mobilen, intelligenten Speicher, insbesondere einer Chipkarte, mit Hilfe eines Endgeräts, das drahtlos mit einem Rechner, vorzugsweise über Rechnerstationen, gesichert kommuniziert, wobei eine gegenseitige dynamische Authentizitätsprüfung zwischen Rechner bzw. Endgerät und Speicher unter Verwendung eines sich ständig ändernden Datenwortes vorgenommen und die Abbuchungsinformation vom Rechner oder Endgerät generiert und vom Speicher verarbeitet und quittiert wird, woraufhin das Endgerät ein Bestätigungssignal für die Durchführung des Buchungsvorganges zum Rechner leitet und ggfs. ein Anerkennungssignal für die getätigte Abbuchung erhält.

Eine wichtige Anwendung eines derartigen Verfahrens besteht in der automatischen Gebührenerhebung im Straßenverkehr durch eine drahtlose Kommunikation zwischen einer straßenseitigen Einrichtung (Rechnerstation mit Funkbake - Roadside System, RSS) und einer fahrzeugseitigen Ausrüstung (On-Board-Unit, OBU, mit Chipkarte, ICC). Das im Fahrzeug befindliche, mit einer Chipkarte bestückbare Endgerät (OBU) wird in einer bekannten Anordnung als Transponder ausgeführt. Die OBU entnimmt dabei dem empfangenen Signal der Funkbake des RSS die erforderliche Energie und sendet an die Funkbake ein mit einem Datenstrom moduliertes Signal zurück.

Es sind zahlreiche Buchungssysteme mit Chipkarten bekannt, bei denen der Buchungsvorgang gesichert durch eine gegenseitige

Authentizitätsprüfung zwischen Endgerät und Chipkarte abläuft. Dabei wird zunächst vom Endgerät ein Buchungssignal erzeugt, durch das die Buchungsapplikation auf der Chipkarte selektiert wird. Nach Erhalt der Bestätigung der vorgenommenen Selektion durch die Chipkarte generiert das Endgeräte eine Zufallszahl und überträgt diese auf die Chipkarte. Die Chipkarte bildet mit der abgespeicherten Signatur unter Verwendung der Zufallszahl eine Kennung, die auf das Endgerät übertragen wird. Das Endgerät extrahiert aus dem Signal die Signatur der Chipkarte und kann somit erkennen, daß die Chipkarte für den Betrieb mit dem jeweiligen Endgerät autorisiert ist. Zur umgekehrten Authentizitätsprüfung generiert nunmehr die Chipkarte eine Zusatzzahl und überträgt diese auf das Endgerät. Der mit dem Endgerät kommunizierende Rechner bildet mit der Zufallszahl und einer eigenen Signatur eine Kennung, die von der Chipkarte empfangen und überprüft wird. Nachdem nunmehr die gegenseitige Authentizität festgestellt worden ist, wird von dem Rechner über das Endgerät der Börsenstand der Chipkarte abgefragt. Aus den erhaltenen Daten wird ein neuer Börsenstand berechnet und über ein Schreibsignal in die Chipkarte eingelesen. Der Einlesevorgang wird von der Chipkarte quittiert und das Quittungssignal auf den Rechner übertragen. Ggfs. veranlaßt das Gerät ein erneutes Auslesen des nunmehr aktuellen Börsenstandes, um diesen mit dem errechneten Börsenstand zu vergleichen.

Dieses Buchungsverfahren setzt sömit mindestens 6 Übertragungen in beiden Richtungen voraus. Der Buchungsvorgang dauert dabei mehrere 100 ms, was im allgemeinen unkritisch ist, da regelmäßig genügend Zeit zur Verfügung steht und die gegenseitigen Übertragungen in der Zeitspanne nicht durch Unterbrechungen gefährdet sind.

Eine völlig andere Situation ergibt sich jedoch für manche Anwendungen, insbesondere für die Gebührenerfassung bei schnellfahrenden Fahrzeugen. Die Mikrowellen-Funkverbindung zwischen dem Fahrzeuggerät und der straßenseitigen stationären Funkbake kann unterbrochen werden und muß darüber hinaus in

einer sehr geringen Zeitspanne abgeschlossen sein. Die gesamte Zahlungstransaktion muß in einem kurzen Zeitrahmen zwischen 50 und 100 ms abgeschlossen sein. Darüber hinaus ist die Kommunikation zwischen dem Endgerät und der Chipkarte nur möglich, wenn eine Funkverbindung mit der Funkbake besteht, wenn das Endgerät als Transponder ausgeführt ist und daher die Energieversorgung aus den empfangenen Signalen der Funkbake entnimmt.

Hieraus resultiert, daß auch die Kommunikation zwischen Endgerät und Chipkarte während des Abbuchungsvorganges anfällig gegenüber Störungen der Funkverbindung ist. Für einen Hochgeschwindigkeits-Buchungsvorgang ist es daher von eminenter Bedeutung, daß die Kommunikation zwischen Endgerät und Chipkarte in einem möglichst kurzen Zeitraum erfolgt, da eine Unterbrechung des Kommunikationsablaufs entweder erfordert, daß die Wiederaufnahme der Kommunikation am gleichen Endgerät erfolgt oder daß alle Endgeräte miteinander vernetzt sind. Beide Voraussetzungen sind beispielsweise bei Gebührenerfassungssystemen für den öffentlichen Personennahverkehr regelmäßig nicht erfüllt.

Die vorliegende Erfindung geht somit von der Problemstellung aus, ein Verfahren zur Durchführung eines Buchungsvorganges der eingangs erwähnten Art anzugeben, das eine Hochgeschwindigkeits-Abwicklung erlaubt und eine nur kleine gegen Unterbrechungen empfindliche Zeitspanne aufweist.

Ausgehend von dieser Problemstellung ist ein Verfahren der eingangs erwähnten Art dadurch gelöst, daß vor einer gegen Unterbrechungen empfindlichen Zeitspanne ein zur dynamischen Authentizitätsprüfung generiertes erstes Datenwort vom Speicher auf das Endgerät übertragen wird,
daß während der gegen Unterbrechungen empfindlichen Zeitspanne vom Endgerät auf den Speicher ein einziges Signal übertragen wird, das ein Buchungsauslösesignal, einen Buchungsdatensatz, eine unter Verwendung des vorher übertragenen ersten Daten-

worts generierte Kennung und ein zweites vom Endgerät generiertes zweites Datenwort enthält, woraufhin der Speicher die Kennung prüft, die Buchung gemäß dem Buchungsdatensatz vornimmt, eine eigene Kennung unter Verwendung des zweiten Datenworts generiert und vom Speicher ein Betätigungssignal für die vorgenommene Buchung zusammen mit seiner generierten Kennung über das Endgerät auf den Rechner übertragen wird, und daß die Bestätigung für die Durchführung der Buchung vom Endgerät auf den Rechner wahlweise innerhalb oder außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne übertragen wird.

Die Erfindung beruht darauf, daß die bisher übliche sequentielle Kommunikation zur gegenseitigen Authentizitätsprüfung, zur Selektion der Applikation und zur Durchführung des Buchungsvorganges in ein einziges Kommandosignal zusammenfaßbar sind. Demgemäß reduziert sich die während der gegen Unterbrechungen empfindlichen Zeitspanne durchgeführte Kommunikation auf ein vom Rechner bzw. Endgerät auf die Chipkarte übertragenes Signal und ein von der Chipkarte zum Rechner bzw. Endgerät zurückübertragenes Signal, das nach den Verarbeitungsvorgängen auf der Chipkarte erzeugt wird. Voraussetzung für diese Kommunikation ist die vorherige Übertragung eines ersten Datenworts vom Speicher auf das Endgerät, wobei das erste Datenwort eine Zeitangabe oder eine Zufallszahl sein kann. Die Komplettierung der Abbuchung kann ferner außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne durch die später erfolgte Bestätigung für die Durchführung der Buchung vom Endgerät an den Rechner erfolgen. Die gegenseitige Authentizitätsprüfung wird regelmäßig zwischen Rechner und Speicher unter Zwischenschaltung des Endgerätes erfolgen. Es ist aber auch denkbar, eine Authentizitätsprüfung nur zwischen Endgerät und Speicher vorzunehmen und lediglich das Ergebnis der Prüfung dem Rechner explizit oder implizit mitzuteilen.

In einer bevorzugten Ausführungsform der Erfindung enthält der Buchungsdatensatz zugleich einen Transaktionsdatensatz zur Erstellung eines Logbucheintrags im Speicher. Auf diese Weise

wird im Speicher ein komplettes Logbuch erzeugt, das alle Vorgänge und Gebührenhöhen dokumentiert.

Zweckmäßigerweise wird der Transaktionsdatensatz im Speicher durch das außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne übertragene Anerkennungssignal vom Rechner ergänzt. Ohne das Anerkennungssignal ist der Transaktionsdatensatz nur vorläufig.

Die vorzugsweise als Speicher verwendeten Chipkarten enthalten häufig nichtflüchtige Speicher (EEPROM), die physikalisch seitenweise organisiert sind. Der Schreibvorgang in einem derartigen Speicher ist zeitaufwendig und jeweils nur für eine Seite möglich. Über der physikalischen Ebene liegt eine logische Organisation in Dateien durch das Chipkarten-Betriebssystem. Die Datei, die die Daten enthält, die von einer Buchung betroffen sind, also üblicherweise eine Datei für eine Geldbörse, ist regelmäßig getrennt von der Logbuch-Datei angelegt. Ein Zugriff auf die Geldbörsen-Datei und die Logbuch-Datei erfordert daher herkömmlich mindestens zwei zeitaufwendige physikalische Schreibzugriffe auf den nichtflüchtigen Speicher. Für den erfindungsgemäßen Zweck einer Hochgeschwindigkeits-Abbuchung ist es daher außerordentlich vorteilhaft, wenn in einer Ausgestaltung des erfindungsgemäßen Verfahrens der (vorläufige) Transaktionsdatensatz auf der Seite abgelegt wird, auf der sich die der Buchung unterliegenden Daten befinden und wenn die Übertragung auf eine Logbuch-Datei außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne erfolgt. Um sicherzustellen, daß diese Übertragung auf die Logbuch-Datei immer erfolgt, kann ein Zustandsautomat auf der Chipkarte implementiert werden, der eine erneute Abbuchung erst nach erfolgreicher Übertragung in die Logbuch-Datei gestattet. Alternativ hierzu kann bei einer erneuten Abbuchung selbständig zuerst die Übertragung des letzten Transaktionsdatensatzes vorgenommen werden. Hiermit wäre allerdings ein Zeitnachteil verbunden.

In heutiger Technik läßt sich der zeitkritische Abbuchungsvorgang zwischen Endgerät und Speicher auf über 150.000 Baud beschleunigen.

Die Erfindung soll im folgenden anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert werden:
Es zeigen:

Figur 1 - eine schematische Darstellung der Kommunikation zwischen einer Funkbake, einer Rechnerstation und einem fahrenden Kraftfahrzeug, das mit einem Endgerät mit einer Chipkarte ausgestattet ist,

Figur 2 - eine schematische Darstellung des für eine Buchung erfindungsgemäß benötigten kompakten Kommunikationsvorgangs zwischen dem Endgerät und der Chipkarte.

Figur 1 läßt eine straßenseitige Rechnerstation 1 mit einer Funkbake 2 erkennen, mit der eine Kommunikation mit einem fahrenden Kraftfahrzeug 3 durchgeführt wird. Hierfür ist das fahrende Kraftfahrzeug mit einem Endgerät OBU ausgestattet, dessen Gebührenguthaben bzw. -kredit auf einer Chipkarte ICC gespeichert ist.

Beim Durchfahren des Kommunikationsbereichs, der im vorliegenden Fall etwa 4,5 m beträgt soll die Straßenbenutzungsgebühr vom Guthaben auf der Chipkarte ICC abgebucht bzw. auf dem Kreditkonto der Chipkarte ICC gebucht werden.

Der hierfür erforderliche Kommunikationsablauf sieht ein Initiierungssignal der Funkbake 2 vor, auf das das Endgerät OBU mit einem "Service Request"-Signal antwortet. Daraufhin erzeugt die Funkbake 2 ein "Debit Order"-Signal, das von dem Endgerät OBU als "Debit Command" auf die Chipkarte ICC übertragen wird. Nach Durchführung der Abbuchung erzeugt die Chipkarte ein Quittungssignal "Receipt", das aufgrund eines Ini-

tiierungssignals der Funkbake 2 von dem Endgerät OBU auf die Funkbake 2 übertragen wird. Den ordnungsgemäßen Erhalt des Quittungssignals bestätigt die Funkbake 2 dann als "Acknowledge" woraufhin das Endgerät OBU das Anerkennungssignal zur Vervollständigung eines Transaktionsdatensatzes auf die Chipkarte überträgt und die Chipkarte die Daten für den nächsten "Service Request" beim Endgerät OBU bereitstellt.

Der zeitkritische Teil dieser Kommunikation liegt zwischen der Erstellung der "Debit Order" durch die Funkbake 2 bis zum Übertragen des Anerkennungssignals auf das Endgerät OBU.

Diese störanfällige Kommunikation wird erfindungsgemäß innerhalb kürzester Zeit dadurch durchgeführt, daß gemäß Figur 2 von dem Endgerät OBU ein MAKRO-Signal auf die Chipkarte ICC übermittelt wird, das ein Selektionssignal für die betreffende Applikation APPL (Buchung), ein Buchungsauslösesignal CMD, den Buchungsbetrag B, die eigene Signatur S1 und eine generierte Zufallszahl R2 enthält. Vorzugsweise enthält das MAKRO-Signal ferner noch einen vorläufigen Transaktionsdatensatz L zur Erstellung einer Logbuchinformation in der Chipkarte ICC. Transaktionsdatensatz und Buchungsbetrag B bilden zusammen einen Buchungsdatensatz.

Die Signatur S1 wird dabei vorzugsweise verschlüsselt übertragen, wozu ein erstes Datenwort R1 benutzt wird, das in Form eines Zeitsignals oder einer Zufallszahl vorher von der Chipkarte ICC auf das Endgerät OBU übertragen worden ist.

Die Chipkarte ICC selektiert die Applikation gemäß APPL, prüft die Signatur S1 und den Buchungsbetrag B, berechnet und schreibt den neuen Börsenstand in der Geldbörsendatei sowie die Logbuchinformation L, um so die Buchung vorzunehmen. Ferner berechnet die Chipkarte ICC unter Verwendung des von dem Endgerät OBU generierten zweiten Datenworts R2, das ebenfalls eine Zufallszahl oder eine Zeitinformation ist, eine zweite Kennung mit Hilfe der eigenen Signatur S2.

Die Chipkarte überträgt nach Durchführung dieser Aktionen ein Quittiersignal und die zweite Kennung mit der Signatur S2 auf das Endgerät OBU. Von dem Endgerät OBU wird das Quittiersignal auf die Funkbake 2, also den Rechner 1 übertragen, der so die Authentizität der Chipkarte ICC überprüft und erkennt.

Die Komplettierung des vorläufigen Transaktionsdatensatzes in der Chipkarte ICC erfolgt durch ein Bestätigungssignal des Rechners 1 für den Empfang des Quittungssignals für die durchgeführte Buchung.

Das Anerkennungssignal des Rechners 1 kann dazu verwendet werden, in der Chipkarte eine Übertragung des vorläufig abgelegten Transaktionsdatensatzes in eine Logbuch-Datei vorzunehmen.

Patentansprüche

1. Verfahren zur Durchführung eines Buchungsvorganges auf einem mobilen, intelligenten Speicher (ICC), insbesondere einer Chipkarte, mit Hilfe eines Endgeräts OBU, das drahtlos mit einem Rechner (1), vorzugsweise über Rechnerstationen, gesichert kommuniziert, wobei eine gegenseitige dynamische Authentizitätsprüfung zwischen Rechner (1) bzw. Endgerät (OBU) und Speicher (ICC) unter Verwendung eines sich ständig ändernden Datenworts (R1, R2) vorgenommen und die Abbuchungsinformation vom Rechner (1) oder Endgerät (OBU) generiert und vom Speicher (ICC) verarbeitet und quittiert wird, woraufhin das Endgerät (OBU) ein Bestätigungssignal für die Durchführung des Buchungsvorganges zum Rechner (1) leitet und ggfs. ein Anerkennungssignal für die getätigte Abbuchung erhält, **dadurch gekennzeichnet, daß** vor einer gegen Unterbrechungen empfindlichen Zeitspanne ein zur dynamischen Authentizitätsprüfung generiertes erstes Datenwort (R1) vom Speicher (ICC) auf das Endgerät (OBU) übertragen wird, daß während der gegen Unterbrechungen empfindlichen Zeitspanne vom Endgerät (OBU) auf den Speicher (ICC) ein einziges Signal (MAKRO) übertragen wird, das ein Buchungsauslösungssignal (CMD), einen Buchungsdatensatz (B, L), eine unter Verwendung des vorher übertragenen ersten Daten-

worts (R1) generierte Kennung (S1) und ein zweites, vom Rechner (1) oder Endgerät (OBU) generiertes Datenwort (R2) enthält, woraufhin der Speicher (ICC) die Kennung (S1) prüft, die Buchung gemäß dem Buchungsdatensatz (B, L), vornimmt, eine eigene Kennung (S2) unter Verwendung des zweiten Datenworts (R2) generiert und vom Speicher (ICC) ein Bestätigungssignal für die vorgenommene Buchung zusammen mit seiner generierten Kennung (S2) über das Endgerät (OBU) auf den Rechner (1) übertragen wird, und daß die Bestätigung für die Durchführung der Buchung vom Endgerät (OBU) auf den Rechner (1) wahlweise innerhalb oder außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne übertragen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Buchungsdatensatz (B, L) einen Transaktionsdatensatz (L) zur Erstellung eines Logbuch-Eintrags im Speicher (ICC) umfaßt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Transaktionsdatensatz (L) im Speicher (ICC) durch das außerhalb der gegen Unterbrechungen empfindlichen Zeitspanne übertragene Anerkennungssignal ergänzt wird.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß der Transaktionsdatensatz (L) in einem seitenweise organisierten Speicher während der gegen Unterbrechungen empfindlichen Zeitspanne vorläufig auf der Seite abgelegt wird, auf der sich die der Buchung unterliegenden Daten befinden, und daß die Übertragung auf eine Logbuch-Datei außerhalb der Zeitspanne erfolgt.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß der Speicher (ICC) für einen Buchungsvorgang gesperrt ist, solange eine vorläufig abgelegter Transaktionsdatensatz (L) noch nicht in die Logbuch-Datei übernommen worden ist.

6. Verfahren nach einem der Ansprüche 1 bis 5 zur Abbuchung von Benutzungsentgelten.

7. Verfahren nach Anspruch 6 zur Gebührenerfassung für Kraftfahrzeuge (3).

Zusammenfassung

Bei einem Verfahren zur Durchführung eines Buchungsvorganges auf einem mobilen, intelligenten Speicher (ICC), insbesondere einer Chipkarte, mit Hilfe eines Endgeräts OBU, das drahtlos mit einem Rechner (1), vorzugsweise über Rechnerstationen, gesichert kommuniziert, läßt sich eine Hochgeschwindigkeits-Abbuchung mit einem geringen Unterbrechungsrisiko dadurch realisieren, daß vor einer gegen Unterbrechungen empfindlichen Zeitspanne ein zur dynamischen Authentizitätsprüfung generiertes erstes Datenwort (R1) vom Speicher (ICC) auf das Endgerät (OBU) übertragen wird, daß während der gegen Unterbrechungen empfindlichen Zeitspanne vom Endgerät (OBU) auf den Speicher (ICC) ein einziges Signal (MAKRO) übertragen wird, das ein Buchungsauslösungssignal (CMD), einen Buchungsdatensatz (B, L), eine unter Verwendung des vorher übertragenen ersten Datenworts (R1) generierte Kennung (S1) und ein zweites, vom Rechner (1) oder Endgerät (OBU) generiertes Datenwort (R2) enthält, woraufhin der Speicher (ICC) die Kennung (S1) prüft, die Buchung gemäß dem Buchungsdatensatz (B, L), vornimmt, eine eigene Kennung (S2) unter Verwendung des zweiten Datenworts (R2) generiert und vom Speicher (ICC) ein Bestätigungssignal für die vorgenommene Buchung zusammen mit seiner generierten Kennung (S2) über das Endgerät (OBU) auf den Rechner (1) übertragen wird.

(Figur 2)

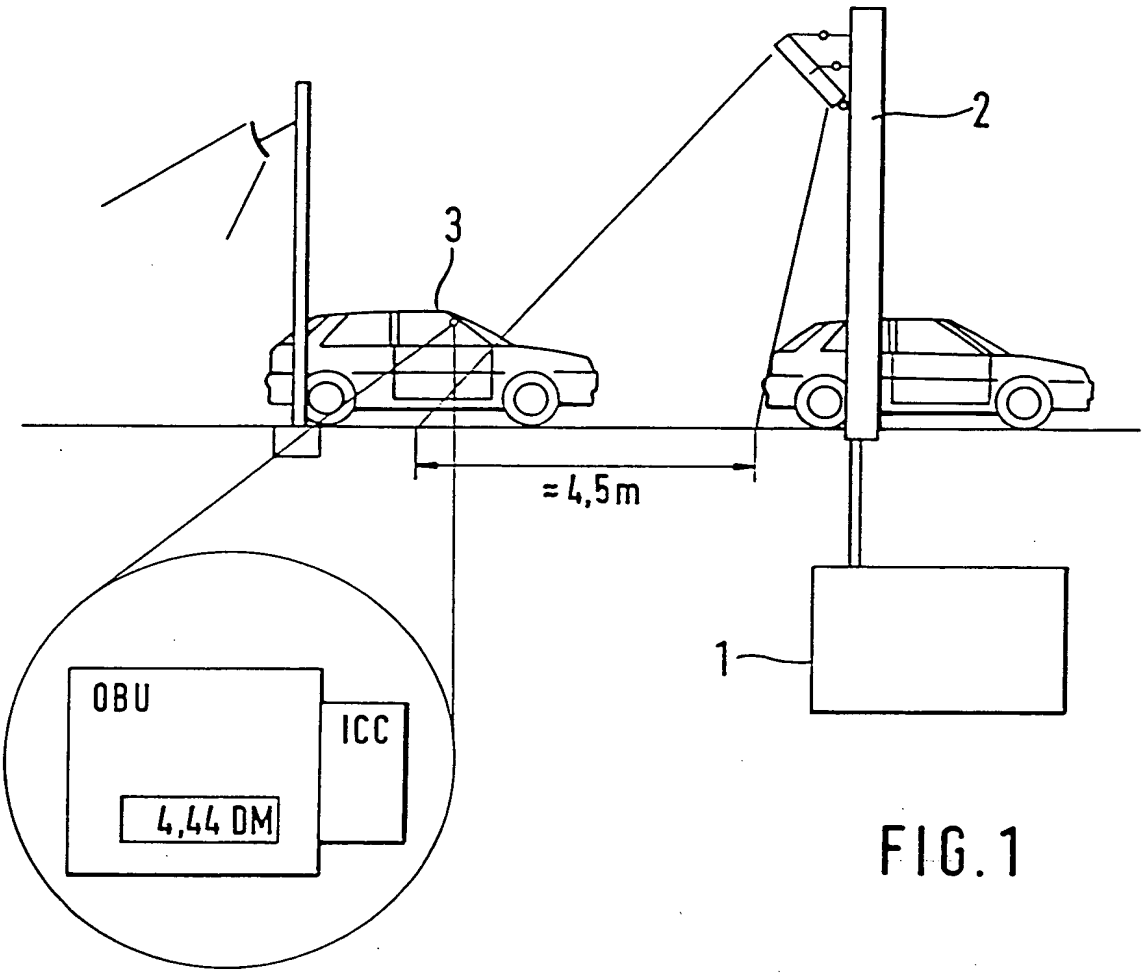


FIG. 1

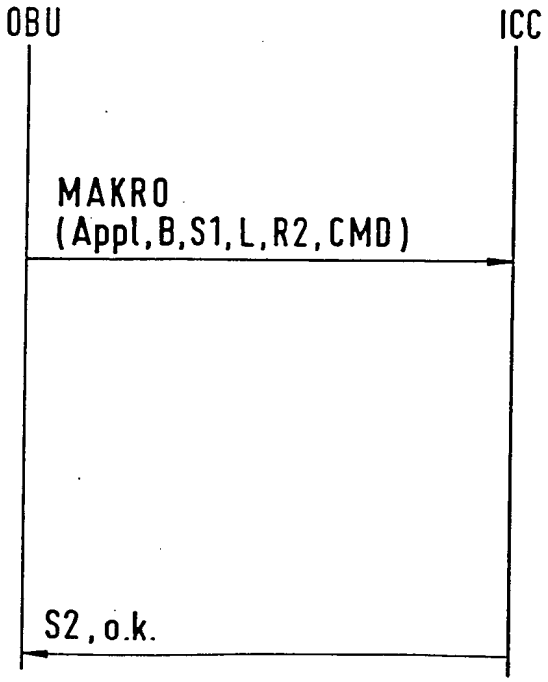


FIG. 2

METHOD OF PERFORMING A POSTING

The present invention relates to a method of performing a posting on a mobile intelligent storage device, in particular an IC card, with the help of a terminal which has secure wireless communication with a computer, preferably via computer stations, with a mutual dynamic authenticity test being performed between the computer or terminal and the storage device using a constantly changing data word, debit posting information being generated by the computer or terminal and processed and acknowledged by the storage device, the terminal subsequently sending a confirmation signal to the computer that the debit posting has been performed and optionally receiving an acknowledgment signal for the posting which has been performed.

One important application of such a method is for automatic collection of tolls and other driving related fees by wireless communication between a roadside system RSS (computer station with a radio beacon) and an on-board unit OBU with an integrated circuit card ICC. The on-board terminal (OBU) in the vehicle can be equipped with an integrated circuit card and is designed as a transponder in a known arrangement. The OBU derives the required energy from the received signal of the RSS radio beacon and sends a signal modulated with a data stream back to the radio beacon.

Numerous posting systems with IC cards are known, with the posting taking place as a secure operation by a mutual authenticity test between the terminal and the IC card. First a posting signal is generated by the terminal, selecting the posting application on the IC card. After receiving confirmation by the IC card that the selection has been performed, the terminal generates a random number and transmits it to the IC card. Using the random number with the stored signature, the IC card forms an identifier and transmits it to the terminal. The terminal extracts the IC

card signature from the signal and can thus recognize that the IC card is authorized for operation with the respective terminal. For reverse authenticity testing, the IC card then generates an additional number and transmits it to the terminal. With the random number and its own signature, the computer communicating with the terminal forms an identifier which is received and verified by the IC card. After mutual authenticity verification, the computer queries the IC card via the terminal to determine the money value carried on the card. A new money value is calculated from the resulting information and entered into the IC card via a write signal. The entry operation is acknowledged by the IC card, with the acknowledgment signal being sent to the computer. The device may optionally cause the new money value to be read out again for comparison with the calculated money value.

This posting method thus presupposes at least six transmissions in both directions. The posting operation requires several hundred ms, which is not generally critical, because usually enough time is available and the mutual transmissions are not at risk of interruptions during this period of time.

However, the situation is completely different for many applications, in particular for collecting tolls from fast-moving vehicles. The wireless microwave connection between the on-board unit and the roadside stationary radio beacon may be interrupted and must be concluded within a very short period of time. The entire payment transaction must be concluded within a short period of time between 50 and 100 ms. In addition, communication between the terminal and the IC card is possible only if there is a radio connection with the radio beacon, if the terminal is designed as a transponder and therefore receives its power supply from the radio beacon signals received.

As a result, communication between the terminal and the IC

card during the debit posting procedure is susceptible to interference in the radio connection. For high speed posting, it is therefore of crucial importance for communication between the terminal and IC card to take place in the shortest possible period of time, because an interruption in communications requires either that communication be resumed with the same terminal or that all terminals be networked. Neither requirement is usually met with toll collecting systems for urban public transportation, for example.

The object of the present invention is thus to provide a posting method of the type mentioned above, which will permit high speed processing and will have only a short period of time during which it is sensitive to interruption.

This problem is solved on the basis of a method of the type defined in the preamble by a first data word, generated for a dynamic authenticity test, being transmitted from the storage device to the terminal before an interrupt-sensitive period of time; a single signal being transmitted from the terminal to the storage device during the interrupt-sensitive period of time, said signal containing a posting triggering signal, a posting data record, an identifier generated using the previously transmitted first data word and a second data word generated by the terminal, whereupon the storage device checks the identifier, performs the posting according to the posting data record and generates its own identifier using the second data word, and an actuating signal for the posting performed is transmitted to the computer together with its generated identifier via the terminal, and confirmation that the posting has been performed is transmitted from the terminal to the computer optionally inside or outside the interrupt-sensitive period of time.

The present invention is based on the fact that the sequential communications that were customary in the past for mutual authenticity testing, for selecting the application and for

performing the posting can be combined into a single command signal. Accordingly, the communication performed during the interrupt-sensitive period of time is reduced to a signal transmitted from the computer or terminal to the IC card and a signal transmitted back from the IC card to the computer or terminal, the latter signal being generated after the processing operations on the IC card. The prerequisite for this communication is prior transmission of a first data word from the storage device to the terminal, with the first data word being either time information or a random number. Furthermore, the debit posting procedure can be completed outside the interrupt-sensitive period of time by the subsequent confirmation for the posting from the terminal to the computer to be performed. The mutual authenticity test is performed regularly between the computer and the storage device with the terminal in between. However, it is also conceivable for an authenticity test to be performed only between the terminal and the storage device and for the computer to only be notified of the result of the test either explicitly or implicitly.

In a preferred embodiment of the present invention, the posting data record also contains a transaction data record for creating a log book entry in the storage device. In this way a complete log book documenting all transactions and fee amounts is generated in the storage device.

The transaction data record in the storage device is advantageously supplemented by the acknowledgment signal from the computer transmitted outside the interrupt-sensitive period of time. Without this acknowledgment signal, the transaction data record is only provisional.

The IC cards preferably used as the storage device often have a non-volatile memory (EEPROM) which is organized physically page by page. Writing to such a memory is time-consuming and is possible only for one page. Above the physical level there

is a logic organization into data files by the IC card operating system. The data file containing the data affected by a posting, i.e., usually a data file for a money account, is usually set up separately from the log book data file. Access to the money account data file and the log book data file therefore traditionally requires at least two time-consuming physical write accesses to the non-volatile storage device. For the purpose of a high speed posting procedure according to the present invention, it is therefore extremely advantageous in one embodiment of the method according to the present invention if the (provisional) transaction data record is stored on the page where the data which is subject to the posting is located and if the transmission to a log book data file takes place outside the interrupt-sensitive period of time. To ensure that this transmission to the log book data file will always take place, an automatic status register may be implemented on the IC card, permitting a new debit posting only after the transfer to the log book data file has been made. As an alternative to this, transmission of the last transaction data record may be performed automatically first when a new debit posting is made. However, this would be associated with a time disadvantage.

With today's technology, the time-critical posting procedure between the terminal and the storage device can be accelerated to more than 150 kbps.

Brief Description of the Drawings

The present invention will be explained in greater detail below on the basis of one embodiment illustrated in the figures, which show:

Figure 1: a schematic diagram of communication between a radio beacon, a computer station and a moving vehicle equipped with a terminal having an IC card;

Figure 2: a schematic diagram of the compact communication between the terminal and the IC card required for a posting according to the present invention.

Detailed Description

Figure 1 shows a roadside computer station 1 with a radio beacon 2 with which it communicates with a moving vehicle 3. For this purpose, the moving vehicle is equipped with an on-board terminal OBU whose fee credit is stored on an integrated circuit card ICC.

When driving through the communication range, which amounts to about 4.5 meters in the present case, the road toll is to be deducted from the credit on IC card ICC, i.e., posted to the credit account of IC card ICC.

The required communication sequence calls for an initiation signal of radio beacon 2, to which terminal OBU responds with a service request signal. Then radio beacon 2 generates a debit order signal which is transmitted from terminal OBU to IC card ICC as a debit command. After the debit posting has been performed, the IC card generates a receipt acknowledgment signal, which is transmitted from terminal OBU to radio beacon 2 on the basis of an initiation signal of radio beacon 2. Proper receipt of the acknowledgment signal is then confirmed by radio beacon 2 as acknowledge whereupon terminal OBU transmits the acknowledgment signal to the IC card to complete a transaction data record, and the IC card makes the information available for the next service request by terminal OBU.

The time-critical part of this communication is from the creation of the debit order by radio beacon 2 until transmission of the acknowledgment signal to terminal OBU.

This communication which is susceptible to interference is

executed within an extremely short period of time according to the present invention due to the fact that a MACRO signal is relayed from terminal OBU to IC card ICC according to Figure 2, with the MACRO signal containing a selection signal for respective application APPL (posting), a posting triggering signal CMD, posting amount B, its own signature S1 and a generated random number R2. Furthermore, the MACRO signal preferably also contains a provisional transaction data record L for creating log book information in IC card ICC. Transaction data record and posting amount B together form a posting data record.

Signature S1 is preferably transmitted in encoded form using a first data word R1 which was previously transmitted from IC card ICC to terminal OBU in the form of a time signal or a random number.

IC card ICC selects the application according to APPL, checks signature S1 and posting amount B, calculates and writes the new money value in the money account data file and log book information L, thereby performing the posting. Furthermore, IC card ICC calculates a second identifier with the help of its own signature S2 using second data word R2 generated by terminal OBU, said data word also being either a random number or time information.

After these operations have been performed, the IC card transmits an acknowledgment signal and the second identifier with signature S2 to terminal OBU. The acknowledgment signal is sent from terminal OBU to radio beacon 2, i.e., to computer 1, which checks and acknowledges the authenticity of IC card ICC.

The provisional transaction data record in IC card ICC is completed by a confirmation signal from computer 1 for receipt of the acknowledgment signal for the posting performed.

The acknowledgment signal from computer 1 can be used to transfer the transaction data record stored in the IC card temporarily to a log book data file.

Patent Claims

1. Method of performing a posting to a mobile intelligent storage device, in particular an IC card (ICC), with the help of a terminal (OBU) engaging in wireless, secure communication with a computer (1), preferably via computer stations, with a mutual dynamic authenticity test being performed between the computer (1), terminal (OBU) and the storage device (ICC) using a constantly changing data word (R1, R2), the debit posting information being generated by the computer (1) or terminal (OBU) and processed and acknowledged by the storage device (ICC), whereupon the terminal (OBU) sends a confirmation signal for performing the posting to the computer (1) and optionally receives an acknowledgment signal for the debit posting thus made, characterized in that before an interrupt-sensitive period of time, a first data word (R1) generated for a dynamic authenticity test is transmitted from the storage device (ICC) to the terminal (OBU); during the interrupt-sensitive period of time, a single signal (MACRO) is transmitted from the terminal (OBU) to the storage device (ICC), said MACRO signal containing a posting triggering signal (CMD), a posting data record (B, L), an identifier (S1) generated using the previously transmitted first data word (R1), and a second data word (R2) generated by computer (1) or terminal (OBU), whereupon the storage device (ICC) checks the identifier (S1), performs the posting according to the posting data record (B, L) and generates its own identifier (S2) using the second data word (R2), said storage device (ICC) then transmitting a confirmation signal for the posting performed together with its generated identifier (S2) to computer (1) via the terminal (OBU), confirmation that the posting has been performed being transmitted from the terminal (OBU) to the computer (1) either inside or outside the interrupt-sensitive period of time.

2. Method according to Claim 1, characterized in that the posting data record (B, L) includes a transaction data record (L) for creating a log book entry in the storage device (ICC).

3. Method according to Claim 1 or 2, characterized in that the transaction data record (L) in the storage device (ICC) is supplemented by the acknowledgment signal transmitted outside the interrupt-sensitive period of time.

4. Method according to Claim 2 or 3, characterized in that the transaction data record (L) is stored temporarily during the interrupt-sensitive period of time on the page in a storage device organized by pages where the data subject to posting is located, and the transmission to a log book data file takes place outside this period of time.

5. Method according to Claim 4, characterized in that the storage device (ICC) is blocked for posting as long as a transaction data record (L) stored temporarily has not been transferred to the log book data file.

6. Method according to one of Claims 1 through 5 for posting use fee debits.

7. Method according to Claim 6 for collecting tolls for motor vehicles (3).

Abstract

In a method of performing posting on a mobile intelligent storage device, in particular an IC card (ICC), with the help of a terminal (OBU) which has wireless, secure communication with a computer (1), preferably via computer stations, a high speed debit posting can be achieved with a low risk of interruption by transmitting a first data word (R1) generated for a dynamic authenticity test from the storage device (ICC) to the terminal (OBU) before an interrupt-sensitive period of time, transmitting a single signal (MACRO) from the terminal (OBU) to the storage device (ICC) during the interrupt-sensitive period of time, said MACRO signal containing a posting triggering signal (CMD), a posting data record (B, L), an identifier (S1) generated using the previously transmitted first data word (R1) and a second data word (R2) generated by the computer (1) or the terminal (OBU), whereupon the storage device (ICC) tests the identifier (S1), performs the posting as per the posting data record (B, L) and generates its own identifier (S2) using the second data word (R2), a confirmation signal for the posting performed being transmitted by the storage device (ICC) together with its generated identifier (S2) to computer (1) via the terminal (OBU).

(Figure 2)

MAKRO -> MACRO